⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平1－152831

⑤1Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　平成1年(1989)6月15日
H 04 L 9/00 11/00	320	Z－7240－5K 7928－5K	

審査請求　未請求　発明の数 1　（全6頁）

⑤4発明の名称　暗号通信処理装置

⑳特　願　昭62－311076
㉒出　願　昭62(1987)12月10日

⑦2発明者　松　永　　宏　長崎県長崎市丸尾町6番14号　三菱電機株式会社長崎製作所内
⑦1出願人　三菱電機株式会社　東京都千代田区丸の内2丁目2番3号
⑦4代理人　弁理士　田澤　博昭　外2名

明　細　書

1．発明の名称

暗号通信処理装置

2．特許請求の範囲

分散型（バス型）ネットワークに接続される複数の端末装置間において暗号文データを送受信する暗号通信処理装置において、当該端末装置のアドレス及び暗号トークンの識別，設定管理を行うアクセス制御回路と、このアクセス制御回路により識別管理された暗号文モードを設定，管理するモード制御回路とを備えたことを特徴とする暗号通信処理装置。

3．発明の詳細な説明

〔産業上の利用分野〕

この発明は、バス形ネットワークに接続する端末装置内で暗号文データを通信する暗号通信処理装置に関するものである。

〔従来の技術〕

従来、情報通信ネットワークまたは端末間通信などにおける暗号文データの通信は、LAN（Local Area Network）などの公衆通信網のような広域で且つ公共性が強い分野で適用されることが多かつた。

この場合、広く不特定多数がネットワークユーザとなるため、システムの保護及び機密保護の立場より、計算機あるいは端末相互間で暗号文データを送受する手続が非常に複雑になつた。

とくに暗号文データに関する公開キーの管理，配送及び暗号文モード，平文モードの切替またはパスワードの認証のための動作手順及び制御が複雑で、システムや装置の効率と操作性が悪く、簡便に適用できなかつた。

第4図は、例えば特開昭61－81043号公報、発明の名称「パケット通信における暗号処理方式」に記載されている従来の暗号文通信方式を示す図である。この図によつて、従来の暗号通信処理装置につきより具体的に説明する。図において、41，42は通信回線、43，44は通信回線41，42を介して通信を行う端末、45，46はそれぞれ各端末43，44の情報組立，分解及

び回線インターフェース機能を有するアダプタ回路、４７，４８はそれぞれ各端末４３，４４の制御プロセッサ、４９，５０はそれぞれ各端末４３，４４の暗号化／復号化回路、５１，５２はそれぞれ各端末４３，４４の暗号キーテーブル、５３，５４はそれぞれ各端末４３，４４の内部バスである。

次に第４図に示した従来の暗号通信処理装置の動作を、第５図に示す情報通信様式を参照して説明する。いま、通信回線４１，４２を経由して端末装置４３，４４が暗号情報の通信を行う場合における動作及び情報通信様式を説明する。端末装置４３が、相手側の端末装置４４へ暗号文を送信する場合、まず、制御プロセッサ４７が、制御手順に従つて、情報組立・分解及び回線インターフェース機能を有するアダプタ回路４５を通じ回線４１，４２及び相手側の端末装置４４との物理的，論理的接続を行う。つぎに制御プロセッサ４７にある送信データが装置の内部バス５３を経由して、暗号化／復号化回路４９及びアダプタ回路４５にラメータを提供する。

受信アドレス識別，発信者識別，鍵識別，データ長識別などはアダプタ回路４６及び制御プロセッサ４８が行い、自己アドレス及び前記各識別子が正しく認識された場合、受信暗号データは暗号化／復号化回路５０にて順次平文データに変換され、内部バス５４を経由して制御プロセッサ４８にあるメモリに取り込まれる。

自己アドレス及び前記識別子が正しく認識されなかつた場合は制御プロセッサ４８によりデータ受信動作を停止し、終了する。

つぎに送信側の端末装置４３が同時に複数の端末装置４４に対してデータを送信する場合の動作を説明する。

送信側の端末装置４３が暗号文送信モードでオペレータまたはプログラムの指示により、暗号文データを複数の端末装置に同時に送信するための同報通信機能が起動されると、宛先アドレスフィールドに暗号文を受信すべき複数の相手側端末装置に共通なアドレスをセットした送信パケットが順次読みだされ、回線へ送出される。このときの送出情報のブロック（以後パケットと呼ぶ）である情報通信様式を第５図に示す。

即ち、第５図において、Ｆはフラグシーケンス、ＦＣＳはフレームチエックシーケンス、Ａはアドレスフイールド、Ｃは制御フイールド、Ｈはデータ長，発信者識別符号，鍵識別符号などを示すヘッダーフイールド、ＤＡＴＡは暗号化データである。

送信側の端末装置４３は、このような送信パケット内に含まれるデータを暗号化／復号化回路49にて暗号化し、また相手側の端末装置４４がそれを復号化し、処理するのに必要な情報を付加したパケットとして回線を通じ、相手側の端末装置44へ送信する。

端末装置４４は到着する受信パケットの送信元の端末装置４３を識別し、該受信パケットに含まれるヘッダーフイールドの情報鍵識別符号にもとづき、自己の鍵テーブル５２から該当鍵をとりだし、復号化回路５０に復号化処理のための関数パ

回線及び相手側の端末装置に対して送出される。

共通アドレスを識別した端末装置は、前記１対１通信の場合と同様、発信者識別，鍵識別，データ長識別を行つた上、暗号データを各々の端末に取り込む。

このようにして暗号文データを複数の端末装置に同時に送信する同報通信が可能となつている。

〔発明が解決しようとする問題点〕

以上説明したように、従来システムにおいて特に暗号文データの同報通信を行う場合、通常の平文データの同報通信の場合と同様に、送信端末装置が受信端末装置群の共通アドレスを送信し、しかして共通アドレスを識別した受信側の各端末装置が受信処理機能を起動することにより実行される。

しかしながらこの場合、前記共通アドレスがエラー発生によつて伝送不要な端末に受取られてしまうことがあり、また受信を期待している端末が確実に暗号文データを受信したか否かを確認することができない問題点があつた。

また従来システムでは、暗号文データの1対1通信を行う場合、平文データと暗号文データの優先制御ができないため、高級管理レベルの秘守データの伝送が遅延する問題点もあつた。

この発明は、以上のような問題点を解消するためになされたもので、信頼性が高く、且つ効率のよい暗号文データ通信の実現をはかることができる暗号通信処理装置を得ることを目的とする。

〔問題点を解決するための手段〕

この発明に係る暗号通信処理装置は、1回線を複数の端末装置で共有する分岐型（バス型）ネットワークにおいて、当該端末装置のアドレス（自局アドレス）及び暗号トークンの識別，設定管理を行うアクセス制御回路と、このアクセス制御回路により識別管理された暗号文モードを設定，管理するモード制御回路とを備えたものである。

〔作　用〕

この発明における暗号通信処理装置では、端末が他の端末との間で暗号文データを送受信する場合、通常の平文データ送受信時のような自由な回線アクセスを抑制し、暗号文データの優先制御を行う。

すなわち、自局アドレス及び更に付加された暗号トークン（暗号文送受信モードフラグ）を受信した端末のみが暗号通信処理モードを起動され、つづいて送られてくる復号化のための暗号キー及び暗号化データを受信処理して暗号文通信の優先制御ができるものである。したがつて当該端末間の暗号文データ通信が継続している間は他の端末による平文データ送受信動作は抑制され、暗号トークン解除フラグを受信したとき、はじめて全端末についての自由な回線アクセスによる平文データの送受信が可能となる。

また、暗号トークンに先だつて宛先共通アドレスを送受信することにより暗号文の優先同報通信を行うこともできる。

〔実施例〕

以下、この発明の一実施例を図について説明する。第1図はこの実施例による暗号通信処理装置の構成を示す。1は伝送路としての通信回線、2，3は回線終端装置、41～4nは前記1本の通信回線1により相互に接続され、分岐型（バス型）のネットワークを形成して通信を行うn台の端末装置，51～5nは各端末装置41～4n内の回線インターフエース回路であつて、前記通信回線1と各端末装置41～4nとを接続してデータ送受信を実行させる回路である。

また、61～6nはアドレス識別と暗号トークンを管理制御するアクセス制御回路、71～7nは端末装置41～4nが平文モード，暗号文モード，暗号文データを複数の端末装置に同時に送信する同報通信モードなど、通信相手との対応で通信制御モードを設定し、管理，制御するモード制御回路、81～8nは端末制御プロセッサ、91～9nは一定のアルゴリズムに従つて平文を暗号文に変換したり、逆に暗号文を平文に変換する暗号処理プロセッサ、101～10nは暗号キーの識別，設定，管理を行うキーテーブルである。111～11nは端末装置の内部バスである。

第2図はこの発明による暗号文データ通信方式における回線上のデータフレーム様式を示す。

Pはビット周期確立のための信号、SFDはフレーム開始を示すコード、ADは宛先アドレス及び発信元アドレス、Lはデータ長、TKは本発明の要点をなす暗号トークン、Kは暗号キー、DATAは送受信情報データ、FCSは伝送誤り検出のためのフレームチエックシーケンスである。

次に、上記実施例の動作を第3図のフローチヤートにより説明する。いま、分岐型（バス型）回線に接続されている端末が他の端末と暗号文データを送受信する場合における受信側端末装置の動作につき説明する。

通常受信モードにある端末装置、例えば4nが他の端末装置、例えば41からアドレスを受信し、ステップST21により自局アドレス指定を認識すると、次につづいて送られてくるフラグコードを受信し識別する。

即ち、本発明の要点をなす暗号トークンフラグがステップST22により認識されると、自局端末装置4nのモードをステップST23により暗

号文データ受信モードにセットする。これによつて本発明の場合、当該端末４ｎは他局からの平文受信、自局の平文送信を受付けない状態となり、以後暗号文データ受信処理の動作を突行する。ステップＳＴ２４～２６が以上の各処理を示す。

即ち、通信回線１を経由して受信するデータは、まず回線インターフエース回路５ｎによつてビット周期をとり、データフレームの開始を示すコードＳＦＤ，アドレスＡＤ，データ長を示すコードＬ，暗号トークンＴＫ，暗号文を平文に復号化するための暗号キーＫ，暗号文データＤＡＴＡ，伝送誤り検出のためのフレームチエックシーケンスＦＣＳ、の順序で受信する。しかして、このうちアドレス識別管理及び暗号トークンの識別管理はアクセス制御回路６ｎで行い、暗号モードにおける通信相手端末装置との間で暗号文データの送受信が終了するまで他局及び自局の平文データ送受信アクセスを禁止する。そして暗号文データの受信処理は端末装置４ｎの内部バス１１ｎを通じて行われ、その基本動作は端末制御プロセッサ８ｎからの暗号文データ送信終了を示す暗号トークン解除コード$\overline{\text{ＴＫ}}$フラグ（$\overline{\text{ＴＫＦ}}$）を受信すると、ステップＳＴ２７により端末制御プロセッサ８ｎはアクセス制御回路６ｎと辺傍して自局の送信暗号文データの有無をステップＳＴ２８により判断し、なければそれまで保持した暗号文データ受信モードをステップＳＴ２９により解除（リセット）し、他局からの平文データ受信または自局の平文データ送信が可能な状態となる（ステップＳＴ３０）。

他方、ステップＳＴ２８において、自局に他の端末装置へ送信すべき暗号文データがあれば、端末制御プロセッサ８ｎの指示にもとづいて、モード制御回路７ｎはステップＳＴ３１により暗号文データ送信モードを設定し、アクセス制御回路６ｎは暗号トークンを保持する。この状態においては他局及び自局端末装置による平文データ送受信は禁止される。自局が暗号文データ送信モードとなれば、先述の暗号文データ受信モードの場合と同様のデータフレームにより、暗号文データを受信すべき相手側端末装置のアドレス，暗号トークンを送出する。

また、当該端末装置４ｎが同一回線１に接続された他の複数の端末装置に同時に暗号文データを送信する同報通信モードにおいては、端末制御プロセッサ８ｎの指示にもとづいてモード制御回路７ｎは同報通信モードを設定し、アクセス制御回路６ｎは暗号トークンを保持するとともに、同報通信アドレスを生成して暗号トークンをつけた形式で回線インターフエース回路５ｎ，回線１経由で相手側端末へ送信を行う。

しかして、この場合の暗号文データの通信も、先に説明した場合同様にして、自局のアドレスＡＤ，暗号トークンＴＫの解読により、指定したアドレスの端末装置だけに暗号文データが確実に受信され、したがつて指定されていない不要な端末装置が誤つて暗号文データを受信することはない

このようにして、暗号文データ通信またはその同報通信処理を確実に、且つ優先的迅速に行うことができる。

なお、この発明の実施例においては、端末装置

が1つの回線を共有する分散型（バス型）ネットワーク構成で、とくに全端末装置が回線を常に自由にアクセスするランダムアクセス・コンテンション（回線争奪）方式であるが、端末装置が相互に送信権を順送りに廻すトークンパッシング方式のネットワークにおいても同じ目的と効果を達成できる。

〔発明の効果〕

以上説明したように、この発明によれば、暗号通信処理装置を、分散型（バス型）ネットワークにおいて、暗号文データを送受信する端末装置の自局アドレス及び暗号トークンを有する暗号文データによつて、該暗号文データの通信処理を行うように構成したから、暗号文データの送受信が優先的に、且つ高信頼度で確実に行えるようになる効果がある。また、暗号文データの同報通信についても効率の良い、且つ信頼度の高い通信処理を実現できるものである。

4. 図面の簡単な説明

第1図はこの発明の一実施例による暗号通信処理装置の構成図、第2図は上記実施例による暗号文データ通信方式における回線上のデータフレーム様式図、第3図は暗号文データ受信モードの動作を説明するフローチャート、第4図は従来の暗号通信処理装置の構成図、第5図は同データフレーム様式図である。

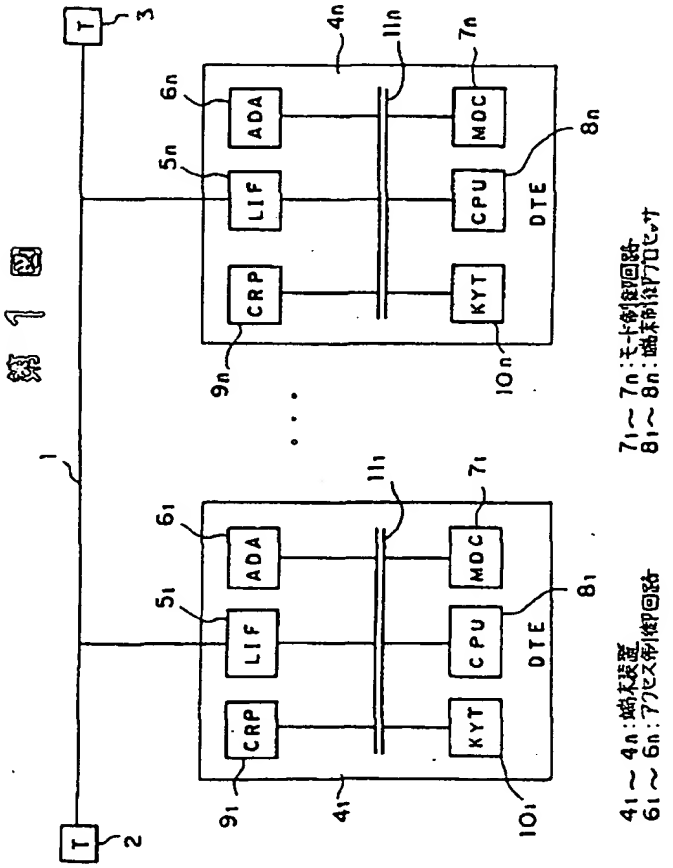
図面中、1は通信回線、41～4nは端末装置、51～5nはインターフェース回路、61～6nはアクセス制御回路、71～7nはモード制御回路、81～8nは端末制御プロセッサ、91～9nは暗号処理プロセッサ、101～10nは暗号キーテーブル、第2図におけるADはアドレス、TKは暗号トークンである。

特許出願人　三菱電機株式会社

代理人　弁理士　田澤博昭

（外2名）

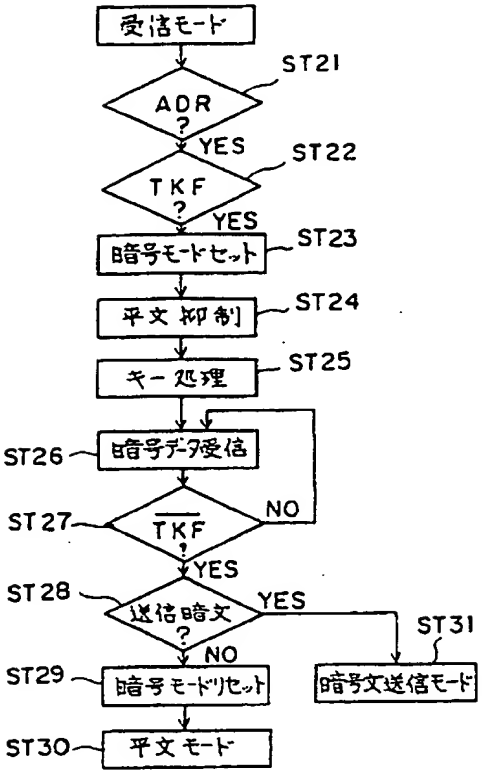
第1図



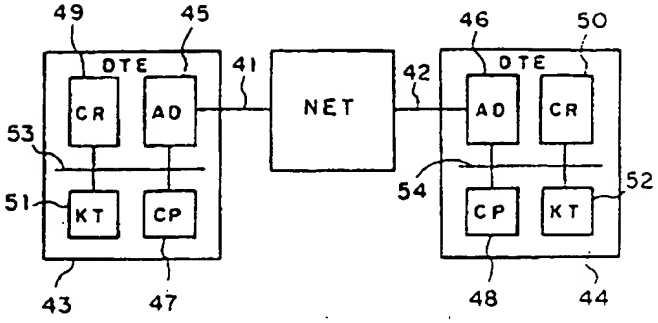
第2図

P	SFD	AD	L	TK	K	DATA	FCS

第 3 図


受信モード
ST21
ADR ?
YES
ST22
TKF ?
YES
暗号モードセット
ST23
平文抑制
ST24
キー処理
ST25
ST26
暗号データ受信
ST27
TKF ?
NO
YES
ST28
送信暗文 ?
YES
ST31
NO
ST29
暗号モードリセット
暗号文送信モード
ST30
平文モード

第 4 図


49
45
DTE
CR
AD
41
NET
42
46
50
DTE
AD
CR
53
51
KT
CP
54
52
CP
KT
43
47
48
44

第 5 図


F
A
C
H
DATA
FCS
F